(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 November 2001 (29.11.2001)

PCT

(10) International Publication Number
WO 01/90859 A1

(51) International Patent Classification⁷: G06F 1/00

(21) International Application Number: PCT/US00/13890

(22) International Filing Date: 19 May 2000 (19.05.2000)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: NETSCAPE COMMUNICATIONS CORPORATION [US/US]; 501 E. Middlefield Road, Mountain View, CA 94043 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: ROSKIND, Jim [US/US]; 920 Governors Bay Drive, Redwood City, CA 94065 (US). WARD, Rory [IE/US]; 334 Schroeder Street, Sunnyvale, CA 94086 (US).

(74) Agents: GLENN, Michael, A. et al.; Glenn Patent Group, 3475 Edison Way, Suite L, Menlo Park, CA 94025 (US).

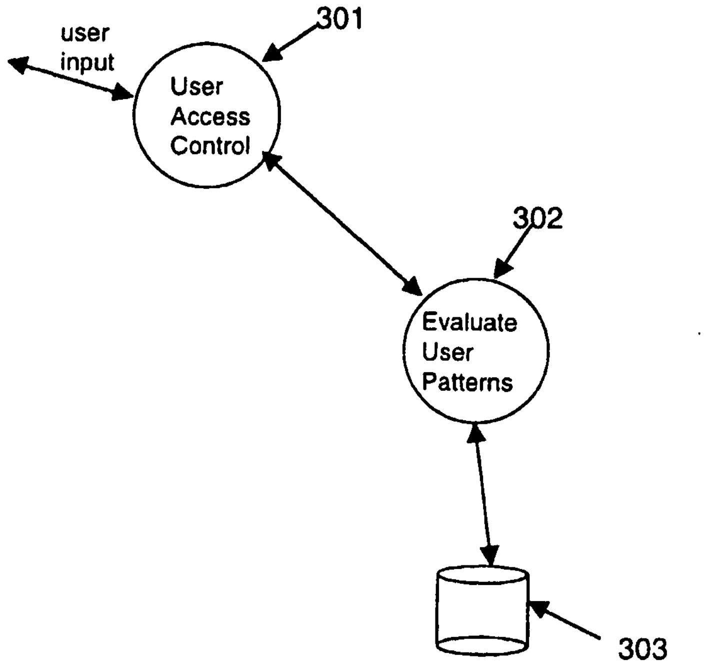
(81) Designated States *(national)*: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: ADAPTIVE MULTI-TIER AUTHENTICATION SYSTEM



(57) Abstract: An adaptive multi-tier authentication system provides secondary tiers of authentication which are used only when the user attempts a connection from a new environment. The invention accepts user input such as login attempts and responses to the system's questions. User login information such as IP address, originating phone number, or cookies on the user's machine are obtained for evaluation. User/usage profiles are kept for each user and the user login information is compared to the information from the user/usage profile for the specific user which contains all of the user information that the user used to establish the account and also the usage profile detailing the user's access patterns. The trust level of the current user login location is calculated and the invention determines if any additional questions to the user are required. If the trust level is high, then the user is granted access to the system. If the trust level is not high enough, then questions are sent to the user and the user's answers are evaluated and access is granted or denied based on the trust level and answers. The user's profile is updated to reflect the access attempt.

WO 01/90859 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Adaptive Multi-Tier Authentication System

BACKGROUND OF THE INVENTION

TECHNICAL FIELD

The invention relates to user access in a computer environment. More particularly, the invention relates to adapting a secure user login from different originating clients in a computer environment.

DESCRIPTION OF THE PRIOR ART

Users commonly have their passwords compromised (lost or stolen). Attackers can typically use the stolen username/password to impersonate a user from a remote site. This compromises the service that the attackers infiltrate, which is costly to the service providers.

Most companies allow users access to an Intranet with very little authentication (*i.e.*, a minor password). This is an extreme case where the company knows where the user is coming from; the access point of the user is in an expected area (*e.g.*, inside the company building). When a user accesses a company's Intranet from an unexpected area (*e.g.*, from home), users must use a secure ID (*i.e.* a major password) to access the first level.

Other mechanisms used to identify people such as biometrics (thumb prints, retinal scanners, etc.) are very expensive and hardware intensive. These type of approaches are difficult to install and use. They are also impractical when applied to the Internet.

The most common solution to avoiding vulnerability to password theft is to require that key material be carried to each authentication environment. Sometimes the key material is stored in a smart card, sometimes it is carried in a floppy (perhaps containing private keys). Either method is typically not user friendly and tend to suffer problems with the loss of the non-password material (or the user forgetting to carry the material).

It would be advantageous to provide an adaptive multi-tier authentication system that automatically adapts to the user's login patterns. It would further be advantageous to provide an adaptive multi-tier authentication system that does not require additional hardware from the service provider.

SUMMARY OF THE INVENTION

The invention provides an adaptive multi-tier authentication system. The system automatically adapts to the user's login patterns. In addition, the invention does not require additional hardware from the service provider by using a query-based security system.

A preferred embodiment of the invention provides secondary tiers of authentication which are used only when the user attempts a connection from a new environment. The invention accepts user input such as login attempts and responses to the system's questions.

User login information such as IP address, originating phone number, or cookies on the user's machine are obtained for evaluation. User/usage profiles are kept for each user.

The user login information is compared to the information from the user/usage profile for the specific user. The user/usage profile contains all of the user information that the user used to establish the account and also the usage profile detailing the user's access patterns.

The trust level of the current user login location is calculated and the invention determines if any additional questions to the user are required. If the trust level is high, then the user is granted access to the system. If the trust level is not high enough, then questions are sent to the user. The user's answers are evaluated and access is granted or denied based on the trust level and answers. The user's profile is updated to reflect the access attempt.

Other aspects and advantages of the invention will become apparent from the following detailed description in combination with the accompanying drawings, illustrating, by way of example, the principles of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block schematic diagram of a user remote access scenario according to the invention;

Fig. 2 is a block schematic diagram of a multiple access point example according to the invention; and

Fig. 3 is a block schematic diagram of a task viewpoint of the invention according to the invention.

DETAILED DESCRIPTION OF THE INVENTION

The invention is embodied in an adaptive multi-tier authentication system in a computer environment. A system according to the invention automatically adapts to the user's login patterns. In addition, the invention provides a system that does not require additional hardware from the service provider by using a query-based security system.

Users commonly have their passwords compromised (lost or stolen). Attackers can typically use the stolen username/password to impersonate a user from a remote site. This compromises the service that the attackers infiltrate, which is costly to the service providers. The invention makes this type of impersonation more difficult by providing secondary tiers of authentication which are used ONLY when the user attempts a connection from a new environment (*i.e.*, from a new computer, kiosk, etc.).

Referring to Fig. 1, a simple user interface scenario is shown. The user 101 logs onto the server 102. The server retrieves the user's stored use profile 103. The location where the user 101 is accessing the server is checked against the user's profile to determine a trust level for the session. The server 102 determines if any additional security measures must be taken based on the trust level.

A preferred embodiment of the invention analyzes the user's use of a service and typical access points to augment the trust level of each access point. If the user is always dialing in from home to access a service such as AOL, the invention observes the pattern and, after a while, determines that the trust level is high when the user accesses the service from home. At that point, the invention will allow immediate login into the service without asking for any additional information.

When the user suddenly goes travelling and accesses the service on the road, then the user's trust level is downgraded and more authentication questions are asked before allowing access. For example, the service may tell the user "We are surprised to see you dialing in from California. We just need to do a little extra background check on your identity. How many dogs did you tell us that you have? What are their names?"

With respect to Fig. 2, the user may be a salesperson and travels to different cities. This user's patterns may be random at best because his access points are all across the country 201, 202, 203. The server 204 takes this into account and determines that this is the user's normal pattern. The server 204 records this fact in the user's profile 205.

However, if the user logs in to the server 204 at one location 201 and then another user logs in using the same identity at another location 203, the server 204 will immediately downgrade the trust level of the second location and ask more authentication questions. This also applies to the situation when a user logs in the United States, for example, and a similar login occurs in Japan five hours later. The invention knows that the time frame is improbable.

The invention automates the process of tracking information such as IP addresses, where the user dialed in from, and the access times. A profile of the combination of data is used to as a basis to determine the level of trust. For example, the invention uses the following criteria to adapt authentication for a system:

- Where the user is dialing in from (*e.g.*, phone number).
- Type of machine being used (*e.g.*, Mac or PC).
- Operating system on the machine.
- Cookies/tags that are on the machine.
- IP address (*e.g.*, same IP address or same subnet).

When a user logs on, some distinct aspect of the computer is recorded. In the typical case, a random token is written into memory, or onto the disk of the client computer. Logon proceeds as usual ONLY if the existing token is located on the computer used for the login (*e.g.*, an identifying cookie would be used on a per-computer basis for HTTP transactions). When the element that is used to identify the computer does not match the user's "standard list of computers used" then some secondary questions are asked as described above (*e.g.*, "What is your birthday?", "What is your home phone number?") before completing the authentication.

The system adapts and leams new sites that the user logs in from, and then proceeds to use the minimal username/password from those sites only. Other techniques could be used to identify the logon environment as listed above (*i.e.*, IP address or dial in line), but the creation of a unique mark (file, cookie, etc.) ensures verification of the environment.

The user is not burdened with having to carry anything with him that could to be lost or stolen (*e.g.*, smart cards). This approach is analogous to traditional human identification systems, where, when the user is known, then additional proof of ID is not requested.

The user immediately knows when something is wrong when the invention suddenly asks for more information than usual. For example, if the user logs in from home, which is a normal situation, and the system asks for more information than normal, such as the user's dog's name. The unusual request would be an indicator to the user that something may be wrong, prompting the user to call into customer support to get more information.

Referring to Fig. 3, the User Access Control module 301 accepts user input such as login attempts and responses to the system's questions. The User Access Control module 301 has the responsibility to search and check for information such as IP address, originating phone number, or cookies on the user's machine. The Evaluate User Pattems module 302 takes the information obtained from the User Access Control module 301 and compares it to the usage information from the user/usage profile 303 for the specific user. The user/usage profile contains all of the user information that the user used to establish the account and also the usage profile detailing the user's access pattems.

The trust level of the current user login location is calculated and the Evaluate User Patterns module 302 determines if any additional questions to the user are required. Questions are sent through the User Access Control module 301 to the user. The user's answers are relayed from the User Access Control module 301 back to the Evaluate User Patterns module 302. The Evaluate User Patterns module 302 grants or denies access based on the trust level and answers for any questions that it asked. The Evaluate User Patterns module 302 updates the user/usage profile 303 for the user with the information just obtained.

Although the invention is described herein with reference to the preferred embodiment, one skilled in the art will readily appreciate that other applications may be substituted for those set forth herein without departing from the spirit and scope of the present invention. Accordingly, the invention should only be limited by the Claims included below.

CLAIMS

1. A process for an adaptive secure access system in a computer environment, comprising the steps of:

receiving user input;

accessing information related to a user login request;

said user login information includes, but is not limited to where the user is dialing in from, the type of machine being used, the operating system on said machine, cookies/tags that are on said machine, and IP address;

providing a plurality of user/usage profiles;

said profiles includes information relating to user login patterns, user personal information, and trust levels for access locations;

comparing said user login information to the information from the user/usage profile for the specific user;

determining a trust level for the current user login location; and

updating the user/usage profile for the user.

2. The process of Claim 1, wherein said determining step recognizes and identifies user login patterns.

3. The process of Claim 1, further comprising the step of:

installing a cookie/tag onto the machine that the user is logging in from.

4. The process of Claim 1, wherein if said trust level is low, then issuing questions to the user relating to the user's personal information.

5. The process of Claim 4, wherein if said questions are answered correctly, then granting access to the user.

6. The process of Claim 4, wherein if said questions are answered incorrectly, then denying access to the user.

7. The process of Claim 1, wherein if said trust level is high, then granting access to the user.

8. An apparatus for an adaptive secure access system in a computer environment, comprising:

a module for receiving user input;

a module for accessing information related to a user login request;

said user login information includes, but is not limited to where the user is dialing in from, the type of machine being used, the operating system on said machine, cookies/tags that are on said machine, and IP address;

a plurality of user/usage profiles;

said profiles includes information relating to user login patterns, user personal information, and trust levels for access locations;

a module for comparing said user login information to the information from the user/usage profile for the specific user;

a module for determining a trust level for the current user login location; and

a module for updating the user/usage profile for the user.

9. The apparatus of Claim 8, wherein said determining module recognizes and identifies user login patterns.

10. The apparatus of Claim 8, further comprising:

a module for installing a cookie/tag onto the machine that the user is logging in from.

11. The apparatus of Claim 8, wherein if said trust level is low, then issuing questions to the user relating to the user's personal information.

12. The apparatus of Claim 11, wherein if said questions are answered correctly, then granting access to the user.

13. The apparatus of Claim 11, wherein if said questions are answered incorrectly, then denying access to the user.

14. The apparatus of Claim 8, wherein if said trust level is high, then granting access to the user.

15. A program storage medium readable by a computer, tangibly embodying a program of instructions executable by the computer to perform method steps for an adaptive secure access system in a computer environment, comprising the steps of:

receiving user input;

accessing information related to a user login request;

said user login information includes, but is not limited to where the user is dialing in from, the type of machine being used, the operating system on said machine, cookies/tags that are on said machine, and IP address;

providing a plurality of user/usage profiles;

said profiles includes information relating to user login patterns, user personal information, and trust levels for access locations;

comparing said user login information to the information from the user/usage profile for the specific user;

determining a trust level for the current user login location; and

updating the user/usage profile for the user.

16. The method of Claim 15, wherein said determining step recognizes and identifies user login patterns.

17. The method of Claim 15, further comprising the step of:

installing a cookie/tag onto the machine that the user is logging in from.

18. The method of Claim 15, wherein if said trust level is low, then issuing questions to the user relating to the user's personal information.

19. The method of Claim 18, wherein if said questions are answered correctly, then granting access to the user.

20. The method of Claim 18, wherein if said questions are answered incorrectly, then denying access to the user.

21. The method of Claim 15, wherein if said trust level is high, then granting access to the user.

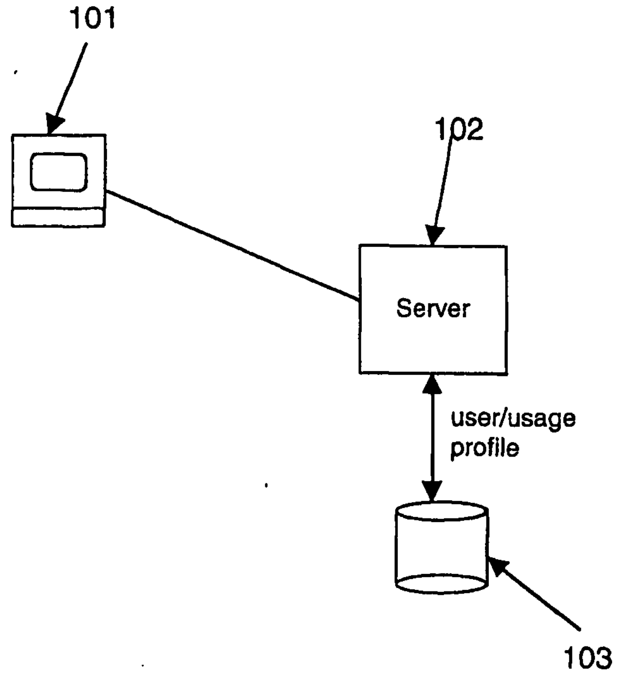


Fig. 1

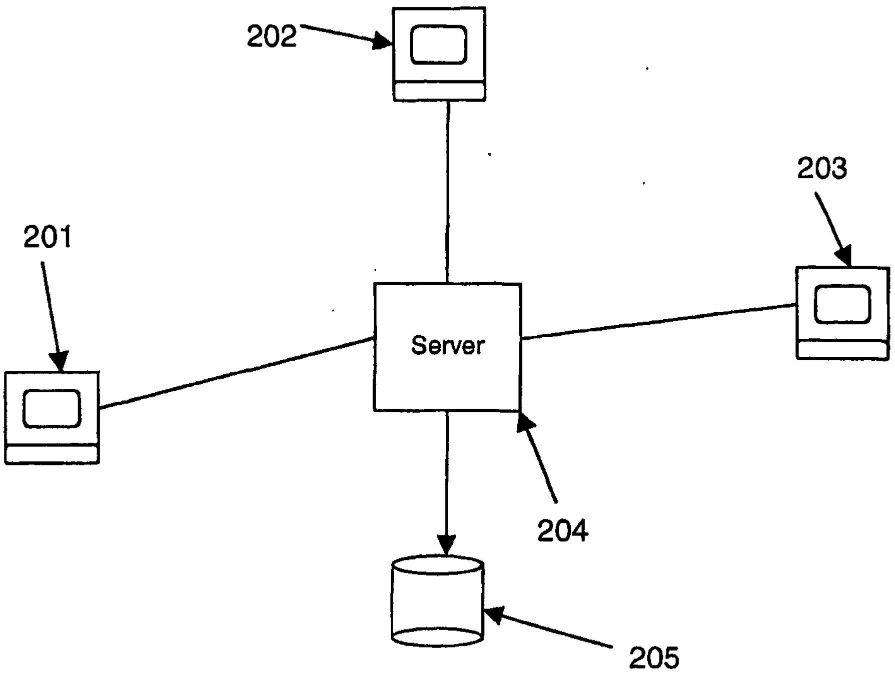


Fig. 2

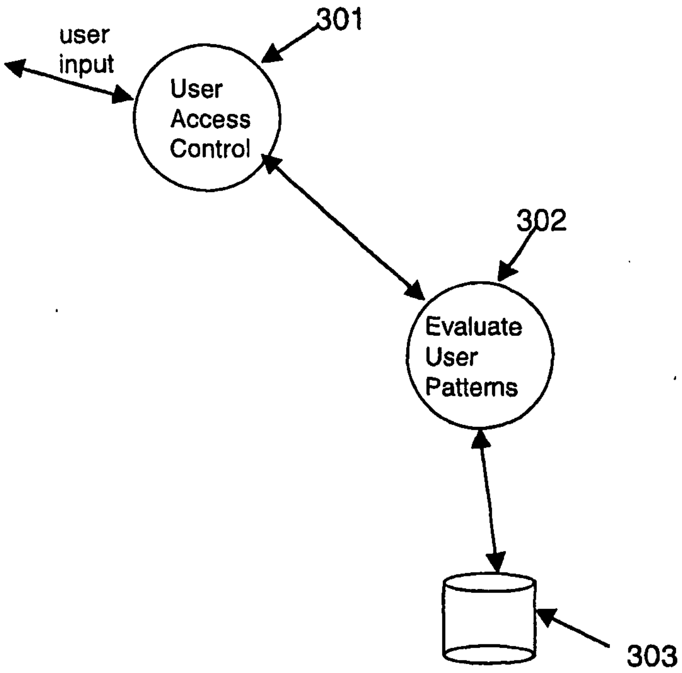

301
user
input
User
Access
Control
302
Evaluate
User
Patterns
303

Fig. 3

INTERNATIONAL SEARCH REPORT

Intern al Application No
PCT/US 00/13890

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 684 951 A (GOLDMAN JONATHAN ET AL) 4 November 1997 (1997-11-04) abstract	1,2,7-9, 14-16,21
A	column 11, paragraph 1 ---	4-6, 11-13, 18-20
Y	WO 99 65207 A (MICROSOFT CORP) 16 December 1999 (1999-12-16) abstract; figures 5,6 page 13, line 3 - line 10 page 14, line 26 -page 16, line 3 page 35, line 7 - line 27 ---	1,2,7-9, 14-16,21
A	US 5 875 296 A (AULT MICHAEL BRADFORD ET AL) 23 February 1999 (1999-02-23) abstract ---	1,3,8, 10,15,17
	-/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 10 January 2001	Date of mailing of the international search report 17/01/2001
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Arbutina, L

INTERNATIONAL SEARCH REPORT

Intern ial Application No
PCT/US 00/13890

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	WO 98 51029 A (SOUTHWESTERN BELL TELEPHONE CO) 12 November 1998 (1998-11-12) page 7, line 13 - line 25 page 11, line 9 - line 21 ---	1,8,15
A	SMITH S L: "AUTHENTICATING USERS BY WORD ASSOCIATION" COMPUTERS & SECURITY. INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY,NL,ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, vol. 6, no. 6, 1 December 1987 (1987-12-01), pages 464-470, XP000050578 ISSN: 0167-4048 page 466, left-hand column, paragraphs 4,5 -----	4,11,18

INTERNATIONAL SEARCH REPORT

Intern al Application No
PCT/US 00/13890

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5684951 A	04-11-1997	NONE	
WO 9965207 A	16-12-1999	NONE	
US 5875296 A	23-02-1999	JP 3003997 B	31-01-2000
		JP 10257048 A	25-09-1998
WO 9851029 A	12-11-1998	NONE	